

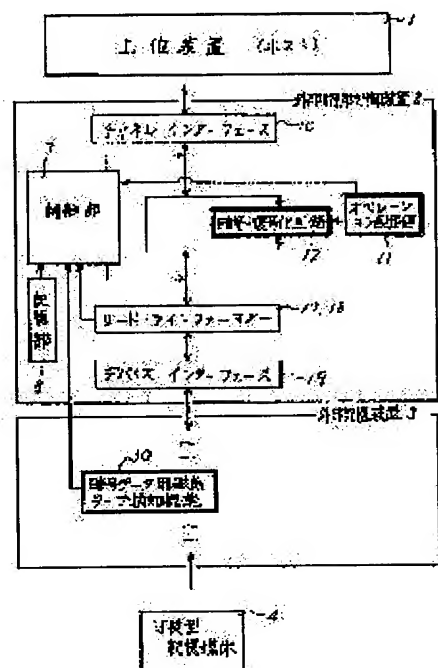
(11)Publication number : 05-165728
(43)Date of publication of application : 02.07.1993

G06F 12/14
G06F 3/06

(71)Applicant : FUJITSU LTD
(72)Inventor : TAKAI NOBUYUKI
KAGAWA KENJI

(57)Abstract:

CONSTITUTION: The external storage sub-system where an external storage device 3 which writes/reads data in the exchangeable storage medium 4 and an external storage controller 2 controlling the external storage device 3 are given, the external storage controller 2 connected to the host device 1 controls the external storage device 3, write data from the host device 1 is written into the exchangeable storage medium 4, data from the exchangeable storage medium 4 is read and it is transferred to the host device 1 which is provided with a ciphering/decoding circuit 12 which ciphers write data from the host device 1 and decodes read data from the external storage device 3 for the external storage controller 2.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-165728

(43)公開日 平成5年(1993)7月2日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 B	9293-5B		
3/06	3 0 4 H	7165-5B		

審査請求 未請求 請求項の数 5 (全 8 頁)

(21)出願番号 特願平3-333283

(22)出願日 平成3年(1991)12月17日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72)発明者 高井 伸幸

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72)発明者 香川 謙治

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

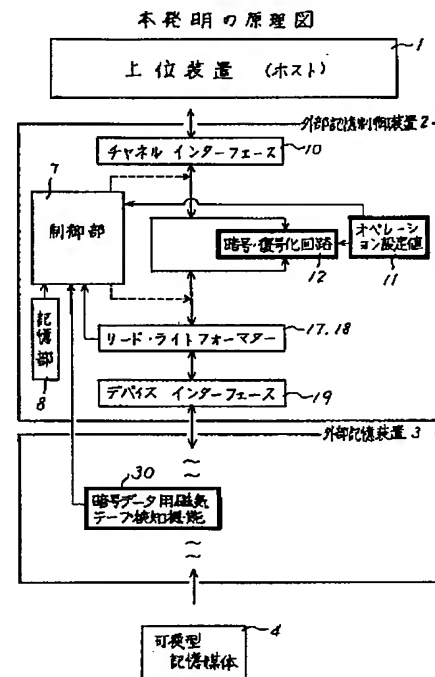
(74)代理人 弁理士 山谷 皓榮

(54)【発明の名称】 外部記憶サブシステム

(57)【要約】

【目的】 磁気テープ等の可換型記憶媒体を用いて、データを暗号化・復号化する外部記憶サブシステムに関し、暗号化・復号化処理に上位装置の負担にならずに、且つ導入がし易いことを目的とする。

【構成】 可換型記憶媒体4の書き込み／読み出しを行う外部記憶装置3と、該外部記憶装置3を制御する外部記憶制御装置2とを有し、上位装置1に接続された該外部記憶制御装置2が該外部記憶装置3を制御して、該可換型記憶媒体4に該上位装置1からの書き込みデータを書き込み、該可換型記憶媒体4からのデータを読み出して、該上位装置1への転送を行う外部記憶サブシステムにおいて、該外部記憶制御装置2に、該上位装置1からの書き込みデータを暗号化し、該外部記憶装置3からの読み出しデータを復号化する暗号化・復号化回路12を設けた。



【特許請求の範囲】

【請求項 1】 可換型記憶媒体（４）の書き込み／読み出しを行う外部記憶装置（３）と、該外部記憶装置

（３）を制御する外部記憶制御装置（２）とを有し、上位装置（１）に接続された該外部記憶制御装置（２）が該外部記憶装置（３）を制御して、該可換型記憶媒体（４）に該上位装置（１）からの書き込みデータを書き込み、該可換型記憶媒体（４）からのデータを読み出して、該上位装置（１）への転送を行う外部記憶サブシステムにおいて、

該外部記憶制御装置（２）に、該上位装置（１）からの書き込みデータを暗号化し、該外部記憶装置（３）からの読み出しデータを復号化する暗号化・復号化回路（１２）を設けたことを特徴とする外部記憶サブシステム。

【請求項 2】 前記外部記憶装置（３）に、前記可換型記憶媒体（４）が暗号用であることを検出する記憶媒体検出手段（３０）を設けるとともに、前記外部記憶制御装置（２）に、前記記憶媒体検出手段（３０）の検出内容に応じて、前記暗号化・復号化回路（１２）を制御する制御部（７）を設けたことを特徴とする請求項 1 の外部記憶サブシステム。

【請求項 3】 前記外部記憶制御装置（２）に、上位装置（１）からの命令により、前記暗号化・復号化回路（１２）を制御する制御部（７）を設けたことを特徴とする請求項 1 の外部記憶サブシステム。

【請求項 4】 前記外部記憶制御装置（２）は、前記外部記憶装置（３）からの読み出しデータにより、暗号化データであるかを判定する判定手段（１７）を有することを特徴とする請求項 2 又は 3 の外部記憶サブシステム。

【請求項 5】 前記外部記憶制御装置（２）に、前記暗号化・復号化回路（１２）の暗号化情報を設定する設定部（１１）を設けたことを特徴とする請求項 1 又は 2 又は 3 又は 4 の外部記憶サブシステム。

【発明の詳細な説明】

【0001】（目次）

産業上の利用分野

従来の技術（図 4）

発明が解決しようとする課題

課題を解決するための手段（図 1）

作用

実施例

(a) 一実施例の説明（図 2 乃至図 3）

(b) 他の実施例の説明

発明の効果

【0002】

【産業上の利用分野】 本発明は、磁気テープ等の可換型記憶媒体を用いて、データを暗号化・復号化する外部記憶サブシステムに関する。

【0003】 近年のコンピュータシステムの発展に伴

い、外部記憶装置の重要機密情報の保護が問題となっているが、磁気テープ、磁気ディスク、光ディスク等の交換可能な可換型記憶媒体は、可換型のため、盗難が可能であり、盗難されると簡単に読み込まれ、データが漏洩してしまう。

【0004】 この重要機密情報のセキュリティの強化の要求に伴い、漏洩防止策として、コンピュータ室の入室管理を強化する方法では、盗難の危険性が皆無とは言えず、盗難されても読めないように、書き込みデータを暗号化して記録し、読み出しデータを復号化する方法が提供されており、コンピュータシステムに導入し易いものが望まれている。

【0005】

【従来の技術】 図 4 は従来技術の説明図である。図 4 に示すように、磁気テープカートリッジ 4 を用いた外部記憶サブシステムは、ホスト（上位装置） 1 と接続された磁気テープ制御装置 2 と、磁気テープ制御装置 2 に制御され、磁気テープカートリッジ 4 に、ホスト 1 の書き込みデータを書き込み、データを読み出す磁気テープ装置 3 とを有する。

【0006】 このようなシステムにおいて、暗号化を行うため、従来ホスト 1 に、暗号化・復号化プログラムを設け、ホスト 1 が、必要なデータを当該プログラムによって、暗号化し、ライトデータを作成して、磁気テープ制御装置 2 に転送し、磁気テープ装置 3 を介し磁気テープ 4 に書き込み、磁気テープ 4 から読み取った暗号化データは、磁気テープ装置 3 より磁気テープ制御装置 2 を介しホスト 1 へ転送し、ホスト 1 の当該プログラムにより、復号化して、データ処理していた。

【0007】

【発明が解決しようとする課題】 しかしながら、従来技術では、次の問題があった。

①暗号化・復号化をホスト 1 のプログラムで実行するため、処理速度が遅いため、外部記憶の入出力処理全てが遅くなる他に、ホスト 1 の負担がかかり、ホストの処理能力低下をきたすおそれがあった。

【0008】 ②ホストの既存の外部記憶の入出力処理全てに、暗号化・復号化機能を追加する作業が必要となり、作業量（工数）が多く、暗号化・復号化機能導入に長時間が必要となる。

【0009】 ③ホストのプログラムは、人為的に作成するため、処理に誤り及び抜けがあると、外部記憶のデータ破壊及び処理障害が生じる。

④暗号化・復号化機能導入後も、新規の記憶媒体の入出力処理にも、暗号化・復号化機能を追加する作業が必要となるため、全体的な運用工数が増加する。

【0010】 ⑤暗号化・復号化機能を追加するに当たり、記憶媒体上のデータが、暗号データか通常データかを判定する機能を新規に作成する必要がある。

従って、本発明は、暗号化・復号化処理に上位装置の負

10

20

30

40

50

担にならずに、且つ導入がし易い外部記憶サブシステムを提供することを目的とする。

【0011】

【課題を解決するための手段】図1は本発明の原理図である。本発明の請求項1は、可換型記憶媒体4の書き込み／読み出しを行う外部記憶装置3と、該外部記憶装置3を制御する外部記憶制御装置2とを有し、上位装置1に接続された該外部記憶制御装置2が該外部記憶装置3を制御して、該可換型記憶媒体4に該上位装置1からの書き込みデータを書き込み、該可換型記憶媒体4からのデータを読み出して、該上位装置1への転送を行う外部記憶サブシステムにおいて、該外部記憶制御装置2に、該上位装置1からの書き込みデータを暗号化し、該外部記憶装置3からの読み出しデータを復号化する暗号化・復号化回路12を設けたことを特徴とする。

【0012】本発明の請求項2は、請求項1において、前記外部記憶装置3に、前記可換型記憶媒体4が暗号用であることを検出する記憶媒体検出手段30を設けるとともに、前記外部記憶制御装置2に、前記記憶媒体検出手段30の検出内容に応じて、前記暗号化・復号化回路12を制御する制御部7を設けたことを特徴とする。

【0013】本発明の請求項3は、請求項1において、前記外部記憶制御装置2に、上位装置1からの命令により、前記暗号化・復号化回路12を制御する制御部7を設けたことを特徴とする。

【0014】本発明の請求項4は、請求項2又は3において、前記外部記憶制御装置2は、前記外部記憶装置3からの読み出しデータにより、暗号化データであるかを判定する判定手段17を有することを特徴とする。

【0015】本発明の請求項5は、請求項1又は2又は3又は4において、前記外部記憶制御装置2に、前記暗号化・復号化回路12の暗号化情報を設定する設定部11を設けたことを特徴とする。

【0016】

【作用】本発明の請求項1では、外部記憶制御装置2に、該上位装置1からの書き込みデータを暗号化し、該外部記憶装置3からの読み出しデータを復号化する暗号化・復号化回路12を設けたので、上位装置1に、暗号化・復号化機能は不要となるので、上位装置の負担とならず、上位装置の入出力処理の遅れも防止でき、上位装置の既存処理の変更が必要なく、導入を短時間ででき、ハード回路で構成しているので、高速処理が可能となり、しかも誤り、障害によりデータ破壊等を防止できる。

【0017】本発明の請求項2では、外部記憶装置3に、前記可換型記憶媒体4が暗号用であることを検出する記憶媒体検出手段30を設けるとともに、前記外部記憶制御装置2に、前記記憶媒体検出手段30の検出内容に応じて、前記暗号化・復号化回路12を制御する制御部7を設けたので、書き込みデータを暗号化するかどうか、読み出しデータを復号化するかどうかを、セットされた可換型記憶媒体により判断できる。

【0018】本発明の請求項3では、外部記憶制御装置2に、上位装置1からの命令により、前記暗号化・復号化回路12を制御する制御部7を設けたので、書き込みデータを暗号化するかどうか、読み出しデータを復号化するかどうかを、上位装置1の命令により判断できる。

【0019】本発明の請求項4では、外部記憶制御装置2は、前記外部記憶装置3からの読み出しデータにより、暗号化データであるかを判定する判定手段17を有するので、読み出しデータにより、暗号化データが自動的に判断できる。

【0020】本発明の請求項5では、外部記憶制御装置2に、前記暗号化・復号化回路12の暗号化情報を設定する設定部11を設けたので、DES、HASH等の暗号方法や暗号キーを、運用に応じて設定できる。

【0021】

【実施例】

(a) 一実施例の説明

図2は本発明の一実施例構成図、図3は本発明の一実施例説明図であり、磁気テープサブシステムを示している。

【0022】図中、図1及び図4で示したものと同一のものは、同一の記号で示してあり、図2において、磁気テープ制御装置2は、ホストインターフェースコントロール部5と、フォーマットコントロール部6とで構成されている。

【0023】10はチャンネルインターフェース部であり、ホスト（上位装置）1のチャンネル1aとのインターフェース制御を行うもの、11はオペレーション設定部であり、オペレータが設定した暗号方法（DES、HASH等）と暗号キーとを設定しておくもの、12は暗号・復号化回路であり、制御部7からの制御により、設定された暗号方法・暗号キーで、書き込みデータを暗号化し、読み出しデータを復号化するもの、13は圧縮・伸長化回路であり、制御部7からの制御により、書き込みデータ（又は暗号化された書き込みデータ）をデータ圧縮し、読み出しデータをデータ伸長するものである。

【0024】14はインターナルバスアダプタであり、内部（インターナル）バス20へデータを送出し、内部バス20のデータを取り込むもの、15はマルチブロックバッファであり、ホストインターフェースコントロール部5側とフォーマットコントロール部6側とのデータ転送速度の吸収のため、データをバッファリングするもの、16はインターナルバスアダプタであり、内部（インターナル）バス20へデータを送出し、内部バス20のデータを取り込むものである。

【0025】17はリードフォーマター部であり、磁気テープ装置3からのフォーマットされているリードデータを分析し、暗号データ、非暗号データ又は圧縮

データ又は非圧縮データであるかを判断し、その結果を制御部7に通知し、磁気テープ用にフォーマットされたリードデータをホスト用データに変換して、ホストインターフェースコントロール部5側に出力するもの、18はライトフォーマター部であり、ライトデータを磁気テープ用にフォーマットし、磁気テープ装置3方向に出力するもの、19はデバイスインターフェース部であり、磁気テープ装置3と磁気テープ制御装置2との間のデータの入出力制御、入出力処理を行うものである。

【0026】7は制御部であり、マイクロプロセッサ(MPU)で構成され、ライトデータの暗号化、非暗号化を判断し、圧縮化、非圧縮化を判断し、各部をライト制御し、リードデータの復号化、非復号化、伸長化、非伸長化を判断し、各部をリード制御するものであり、8は記憶部であり、コントロールストレージを構成し、制御部7が実行する制御プログラム等を格納するものである。

【0027】磁気テープ装置3は、磁気テープドライブ装置で構成され、暗号、圧縮テープ検出機構30を有し、セットされた磁気テープカートリッジ4のリード／ライトを行うものである。

【0028】暗号、圧縮テープ検出機構30は、図3に示すように、磁気テープカートリッジ4に設けた暗号シールS1を検出する暗号センサ30aと、磁気テープカートリッジ4に設けた圧縮シールS2を検出する圧縮センサ30bとを有する。

【0029】尚、磁気テープ4には、図3(B)に示すように、暗号フラグと圧縮フラグが先頭に設けられており、暗号フラグがセットされていると、暗号データが書き込まれている、圧縮フラグがセットされていると、圧縮データが書き込まれていると判断できるようにしている。

【0030】磁気テープドライブ装置3に、磁気テープカートリッジ4がセットされると、暗号・圧縮テープ検出機構30のセンサ30a、30bの出力を、制御部7に通知する。

【0031】これにより、制御部7は、セットされた磁気テープカートリッジ4が、暗号・圧縮用か、暗号・非圧縮用か、非暗号・圧縮用か、非暗号・非圧縮用かを判定する。

【0032】次に、ライト動作について説明する。ホスト1からライトアクセスがあると、チャンネルインターフェース制御部10を介して制御部7に通知され、ライト処理が起動される。

【0033】制御部7は、磁気テープカートリッジ4が、非暗号・非圧縮テープであれば、ホスト1からのライトデータをチャンネルインターフェース制御部10を介し、インターナルバスアダプタ14に直接転送し、バス20、マルチブロックバッファ15よりインターナルバ

スアダプタ16に入力し、ライトフォーマター部18で磁気テープ用にフォーマットし、デバイスインターフェース部19より、磁気テープドライブ装置3に転送し、磁気テープカートリッジ4に書き込む。

【0034】一方、磁気テープカートリッジ4が、暗号・非圧縮テープであれば、制御部7は、オペレーション設定部11の暗号方法情報と暗号キーとにより、暗号・復号化回路12を起動し、ホスト1からのライトデータをチャンネルインターフェース制御部10を介し、暗号・復号化回路12に入力し、設定した暗号方法と暗号キーにより暗号データに変換して、インターナルバスアダプタ14に転送し、バス20、マルチブロックバッファ15よりインターナルバスアダプタ16に入力し、ライトフォーマター部18で磁気テープ用にフォーマットし、デバイスインターフェース部19より、磁気テープドライブ装置3に転送し、磁気テープカートリッジ4に書き込む。

【0035】又、磁気テープカートリッジ4が、暗号・圧縮テープであれば、制御部7は、オペレーション設定部11の暗号方法情報と暗号キーとにより、暗号・復号化回路12を起動し、圧縮・伸長化回路13を起動して、ホスト1からのライトデータをチャンネルインターフェース制御部10を介し、暗号・復号化回路12に入力し、設定した暗号方法と暗号キーにより暗号データに変換した後、圧縮・伸長化回路13に入力し、圧縮データに変換して、インターナルバスアダプタ14に転送し、バス20、マルチブロックバッファ15よりインターナルバスアダプタ16に入力し、ライトフォーマター部18で磁気テープ用にフォーマットし、デバイスインターフェース部19より、磁気テープドライブ装置3に転送し、磁気テープカートリッジ4に書き込む。

【0036】更に、磁気テープカートリッジ4が、非暗号・圧縮テープであれば、制御部7は、圧縮・伸長化回路13を起動して、ホスト1からのライトデータをチャンネルインターフェース制御部10を介し、圧縮・伸長化回路13に入力し、圧縮データに変換して、インターナルバスアダプタ14に転送し、バス20、マルチブロックバッファ15よりインターナルバスアダプタ16に入力し、ライトフォーマター部18で磁気テープ用にフォーマットし、デバイスインターフェース部19より、磁気テープドライブ装置3に転送し、磁気テープカートリッジ4に書き込む。

【0037】次に、リード動作について説明する。ホスト1からリードアクセスがあると、チャンネルインターフェース制御部10を介して制御部7に通知され、リード処理が起動される。

【0038】制御部7は、磁気テープドライブ装置3からの磁気テープカートリッジ4のリードデータをデバイスインターフェース制御部19を介し、リードフォーマター部17に入力し、暗号フラグ、圧縮フラグの分析を

10

20

30

40

50

行わしめ、分析結果を受ける。

【0039】リードフォーマター部17はリードデータをホスト用のデータに直して、インターナルバスアダプタ16に転送し、バス20、マルチブロックバッファ15よりインターナルバスアダプタ14に入力する。

【0040】制御部7は、分析結果により、リードデータが、非暗号・非圧縮であれば、インターナルバスアダプタ14のリードデータを、チャンネルインターフェース部10に直接転送して、ホスト1に転送する。

【0041】一方、制御部7は、分析結果により、リードデータが、暗号・非圧縮であれば、オペレーション設定部11の暗号方法情報と暗号キーとにより、暗号・復号化回路12を起動し、インターナルバスアダプタ14のリードデータを、暗号・復号化回路12に転送し、指定された暗号方法と暗号キーとにより複合データに変換せしめ、チャンネルインターフェース部10に転送して、ホスト1に転送する。

【0042】又、制御部7は、分析結果により、リードデータが、暗号・圧縮テープであれば、制御部7は、オペレーション設定部11の暗号方法情報と暗号キーとにより、暗号・復号化回路12を起動し、圧縮・伸長化回路13を起動して、インターナルバスアダプタ14のリードデータを、圧縮・伸長化回路13に転送して、伸長データに変換した後、暗号・復号化回路12に転送し、指定された暗号方法と暗号キーとにより復号データに変換せしめ、チャンネルインターフェース部10に転送して、ホスト1に転送する。

【0043】更に、制御部7は、分析結果により、リードデータが、非暗号・圧縮テープであれば、圧縮・伸長化回路13を起動して、インターナルバスアダプタ14のリードデータを、圧縮・伸長化回路13に転送して、伸長データに変換した後、チャンネルインターフェース部10に転送して、ホスト1に転送する。

【0044】このようにして、磁気テープ制御装置2に、暗号・復号化回路12を設けたので、上位装置1は、暗号・復号処理をしなくて済み、上位装置1の負担が軽減するとともに、入出力処理に暗号・復号機能を持たせなくて良いので、入出力処理が低下することもなく、複雑なプログラムの変更も必要なく、短期間で導入でき、プログラムによるエラー、障害等も発生せず、データ破壊を防止できる。

【0045】しかも、暗号・復号化回路12は、ハード構成のため、高速処理が可能であり、上位装置1を持たせずに実行できる。又、ライト時は、セットされた磁気テープカートリッジ4から暗号化の有無を判定するので、容易に暗号化、非暗号化の制御を可能とする。

【0046】更に、リード時は、リードデータから、暗号データか否かを判定しているので、確実に判断できる。しかも、オペレータの設定により、暗号方法、暗号キーを設定できるので、数種の暗号・復号化が可能であ

り、ユーザーは、自己のコンピュータセンター特有の暗号・復号化方法を選択でき、より安全性が高い。

【0047】又、圧縮、伸長を同時にできるため、ユーザーの要求に応じたデータ変換が可能となる。

(b) 他の実施例の説明

上述の実施例の他に、本発明は、次のような変形が可能である。

【0048】①リード時に、リードデータから暗号データか否かを判定しているが、そのようなデータを持たない時は、磁気テープカートリッジ4の暗号センサ30aの出力により、判断しても良く、リードデータの分析結果と暗号センサ30aの出力のマッチングを取り、確認しても良い。

【0049】②ライト時に、磁気テープカートリッジ4の暗号センサ30aの出力により、判断しているが、このようなセンサを持たない場合には、上位装置1で暗号化か否かが判るから、上位装置1からの命令により、暗号化するか否か制御しても良く、上位装置1のかかる命令と磁気テープカートリッジ4の暗号センサ30aの出力のマッチングをとり、磁気テープカートリッジ4の誤セットを検出しても良い。

【0050】③又、リード時に、上位装置1はアクセスするファイルにより、暗号化されているか否かを判定できれば、上位装置1の命令により、復号するか否かを判断できる。

【0051】④ライト時及びリード時の暗号・復号指示を、オペレーション設定部11より行っても良い。

⑤外部記憶媒体を、磁気テープで説明したが、可換型の磁気ディスク・光ディスク、光カード、ICメモリ等の可換型記憶媒体にも適用できる。

【0052】以上、本発明を実施例により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【0053】

【発明の効果】以上説明したように、本発明によれば、次の効果を奏する。

①外部記憶制御装置に、暗号・復号化回路を設けたので、暗号・復号化処理を外部記憶制御装置で自動的に実行できるため、上位装置の負担が軽減し、入出力処理の低下を防止できる。

【0054】②上位装置の処理に変更を加える必要がないので、障害等の発生を防止でき、しかも短期間で導入できる。

③暗号・復号化回路が、専用のハード回路のため、高速処理が可能となり、上位装置1を待たせずに、暗号・復号化を実行でき、コンピュータシステムのセキュリティの向上を高速に実行できる。

【図面の簡単な説明】

【図1】本発明の原理図である。

【図2】本発明の一実施例構成図である。

【図3】本発明の一実施例説明図である。

【図4】従来技術の説明図である。

【符号の説明】

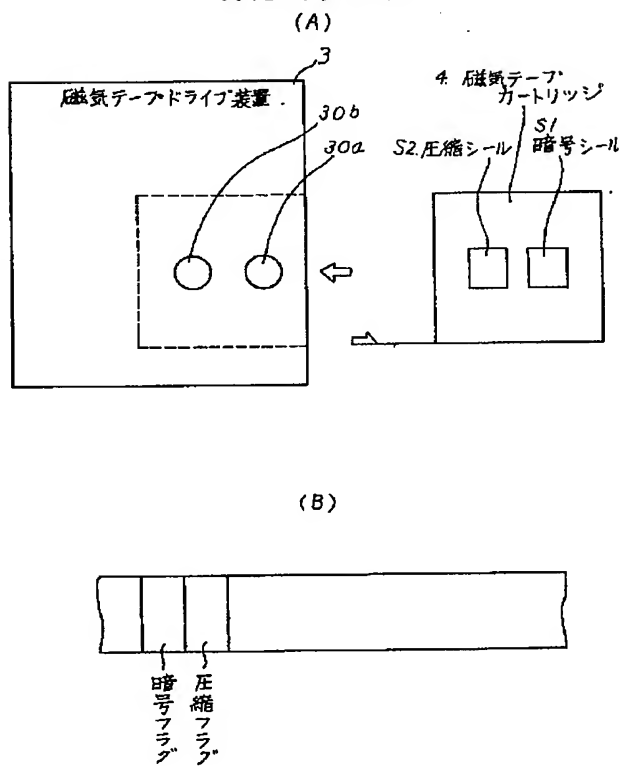
- 1 上位装置 (CPU)
 2 外部記憶制御装置 (磁気テープ制御装置)
 3 外部記憶装置 (磁気テープ装置)
 4 可換型記憶媒体 (磁気テープカートリッジ)
 7 制御部

- * 10 チャンネルインターフェース部
 11 オペレーション設定部
 12 暗号・復号化回路
 17 リードフォーマター部
 18 ライトフォーマター部
 19 デバイスインターフェース部
 30 暗号・圧縮テープ検出機構

*

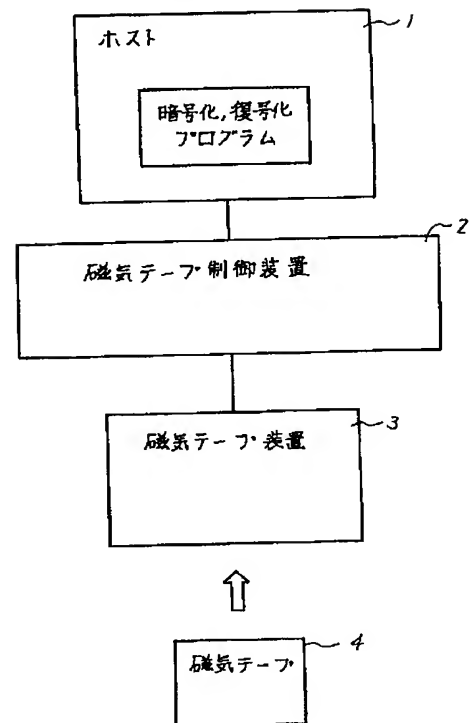
【図3】

一実施例説明図



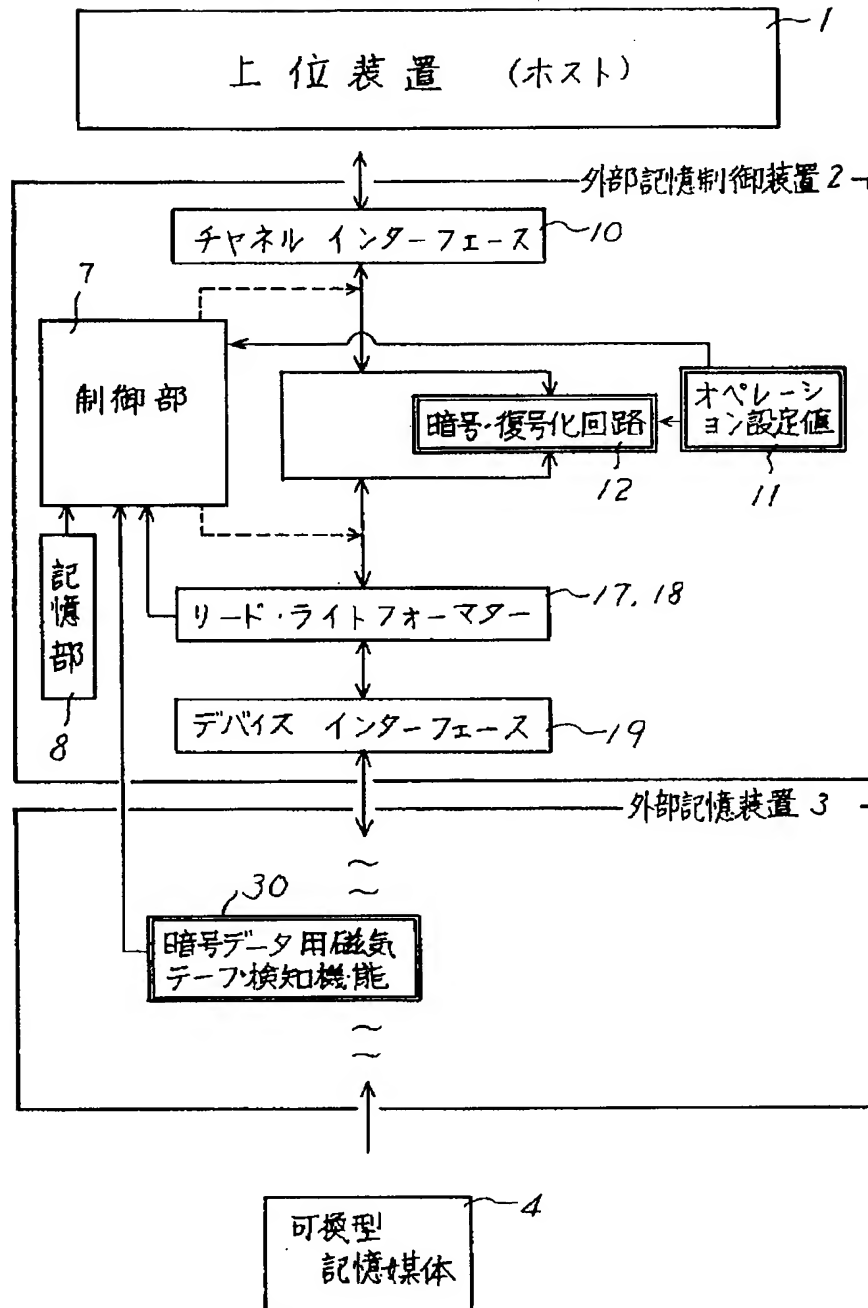
【図4】

従来技術の説明図



【図1】

本発明の原理図



【図2】

一実施例構成図
 ホスト1のチャネル 1a

